0022301940 *Drawing available*
Apparatus for performing hash operation on message blocks to generate message digest in computing environment, has x86-compatible microprocessor with integer unit that executes micro instructions to test bit in flag register
Patent Assignee: VIA TECHNOLOGIES INC (VIAT-N)
Inventor: CRISPIN T A; HENRY G G; PARKS T

Patent Family (1 patents, 1 countries)							
Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
US 20110202775	A1	20110818	US 201110292	A	20110120	201156	B
			US 2003510803	P	20031010		
			US 2004571123	P	20040514		
			US 2004582423	P	20040624		
			US 2004582422	P	20040624		
			US 2004610481	P	20040916		
			US 2004963427	A	20041012		

Alerting Abstract US A1
NOVELTY - The apparatus has a microprocessor i.e. x86-compatible microprocessor, provided with an atomic hash instruction (400) to perform hash operation. A hash mode field (404) coupled to an opcode field (403) prescribes the microprocessor to accomplish the hash operation based on a prescribed hash mode. The microprocessor comprises an integer unit to operate in a parallel direction with a hash unit, where the integer unit executes micro instructions to test a bit in a flag register to update text pointer registers and interrupt process during execution of the hash operation.
DESCRIPTION - An INDEPENDENT CLAIM is also included for a method for performing a hash operation in a microprocessor.
USE - Apparatus for performing a hash operation on message blocks to generate message digest in a computing environment.
ADVANTAGE - The apparatus exhibits superior performance characteristics and provides an opcode value as spare or unused opcode values within an existing instruction set architecture so as to preserve compatibility within a conforming microprocessor with legacy operating system and application software. The apparatus enables hash operations to be resistant to unauthorized observation, supports multiple hash algorithms, mode programmable and verification and testing of the particular hash algorithm, ensures self-preprocessing i.e. self padding, of messages and supports multiple **message** block **sizes** provided for programmable **hash** algorithm modes.

0014743767 *Drawing available*
WPI Acc no: 2005-091393/200510
XRPX Acc No: N2005-079899

Spam message filtering method involves determining whether incoming message is spam based on comparison of uniform resource locator from incoming message with uniform resource locator characterizing spam

Patent Assignee: BRIGHTMAIL INC (BRIG-N); COWINGS D (COWI-I); HOOGSTRATE D (HOOG-I); JENSON S (JENS-I); MEDLAR A (MEDL-I); SCHNEIDER K (SCHN-I)

Inventor: COWINGS D; HOOGSTRATE D; JENSEN S; MEDLAR A; SCHNEIDER K; JENSON S

Patent Family (3 patents, 107 countries)							
Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
WO 2004114614	A1	20041229	WO 2004US19791	A	20040618	200510	B
US 20090070872	A1	20090312	US 2003479754	P	20030618	200920	E
			US 2004871583	A	20040617		
TW 200516893	A	20050516	TW 2004117715	A	20040618	200957	E

Alerting Abstract WO A1

NOVELTY - The data indicative of the uniform resource locator (URL) in the incoming email message is detected. The identified URL in the incoming message is compared with the URL characterizing spam, to determine whether the incoming signal is spam.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
1. system for filtering spam messages;
2. apparatus for filtering spam messages; and
3. recorded medium storing instructions for filtering spam messages.

USE - For filtering spam messages such as unwanted email messages using uniform resource locator (URL) filtering module through network e.g. internet.

ADVANTAGE - Determines and filters spam messages effectively.

02338666
Steganographic method and device
Patent Assignee:
- **Wistaria Trading, Inc.** (2917420)
  16711 Collins Avenue, Suite 2505; Sunny Isles Beach FL 33160 (US)
  (Applicant designated States: all)

Inventor:
- **Cooperman, Marc S.**
  20 Wildwood; Short Hills, NJ 07078; (US)
- **Moskowitz, Scott A.**
  Townhouse 4, 20191 East Country Club Drive; North Miami Beach, FL 33180; (US)

Legal Representative:
- **Vossius & Partner** (100314)
  Siebertstrasse 4; 81675 Munchen; (DE)

	Country	Number	Kind	Date	
Patent	EP	1843507	A2	20071010	(Basic)
Patent	EP	1843507	A3	20071121	
Application	EP	2007112420		19960607	
Priorities	US	489172		19950607	

Abstract EP 1843507 A3
An apparatus and method for encoding and decoding additional information into a steam of digitized samples in an integral manner. The information is encoded using special keys. The information is contained in the samples, not prepended or appended to the sample stream. The method makes it extremely difficult to find the information in the samples if the proper keys are not possessed by the decoder. The method does not cause a significant degradation to the sample stream. The method is used to establish ownership of copyrighted digital multimedia content and provide a disincentive to piracy of such material.

It is important that the hash function be insensitive to any changes in the samples induced by the stega-cipher itself For instance, one might ignore the least significant bit of each sample when computing the hash function, if the stega-cipher was implemented using a least significant bit encode mode.
Based on the **size** of the non-**hash message**, one knows the **hash**-inclusive messagerequires 32 more bytes of space. One can now calculate the size of a signed encrypted copy of this message by signing and encrypting exactly as many random bytes as are in the message, and measuring the size of the output in bytes. One now knows the size of the message to be encoded. One can pre-process the sample stream as follows.

7/9/6 (Item 5 from file: 350)
DIALOG(R)File 350: Derwent WPIX
(c) 2012 Thomson Reuters. All rights reserved.

0015074559 *Drawing available*
WPI Acc no: 2005-423998/200543
XRPX Acc No: N2005-344109
Information processing method for use over e.g. local area network, involves performing hash pattern matching functions on message and accepting message based on pattern match acceptance indicator, when pattern match is detected
Patent Assignee: GREAVES C A (GREA-I); MARTIN H M (MART-I); NGUYEN T Q (NGUY-I); NUNEZ J M (NUNE-I); FREESCALE SEMICONDUCTOR INC (FRSE)
Inventor: GREAVES C A; MARTIN H M; NGUYEN T Q; NUNEZ J M

			Patent Family (9 patents, 107 countries)				
Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
US 20050108943	A1	20050526	US 2003721196	A	20031125	200543	B
WO 2005055487	A2	20050616	WO 2004US37147	A	20041105	200543	E
CN 1879354	A	20061213	CN 200480033180	A	20041105	200730	E
JP 2007512770	W	20070517	WO 2004US37147	A	20041105	200735	E
			JP 2006541232	A	20041105		
KR 2006134937	A	20061228	WO 2004US37147	A	20041105	200744	E
			KR 2006710005	A	20060523		
US 7240041	B2	20070703	US 2003721196	A	20031125	200746	E
TW 200525954	A	20050801	TW 2004136312	A	20041125	200957	E
CN 100534052	C	20090826	CN 200480033180	A	20041105	200965	E
JP 4485529	B2	20100623	WO 2004US37147	A	20041105	201041	E
			JP 2006541232	A	20041105		

Alerting Abstract US A1
NOVELTY - The method involves receiving a message. A hash function and a pattern matching function are performed on the message. A determination of whether a pattern match corresponding to a pattern is detected within the message, by a packet controller (160), where the pattern is indicated by pattern match data. The message is selectively accepted based on a pattern match acceptance indicator, when the pattern match is detected.
DESCRIPTION - An INDEPENDENT CLAIM is also included for a packet controller.
USE - Used for processing information via a network e.g. local area network (LAN) and wide area network (WAN).
ADVANTAGE - The method increases efficiency of message acceptance and rejection without increasing software-based processor tasks and consumption, and enhances the performance of processing incoming messages.